

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-306301

(43) 公開日 平成11年(1999)11月5日

(51) Int.Cl.⁸

識別記号

F I

G 0 6 K 17/00
19/07
19/073

G 0 6 K 17/00
19/00

S
N
P

審査請求 未請求 請求項の数4 O L (全 5 頁)

(21) 出願番号

特願平10-110924

(22) 出願日

平成10年(1998)4月21日

(71) 出願人 000002897

大日本印刷株式会社

東京都新宿区市谷加賀町一丁目1番1号

(72) 発明者 矢野義博

東京都新宿区市谷加賀町一丁目1番1号大

日本印刷株式会社内

(72) 発明者 半田富己男

東京都新宿区市谷加賀町一丁目1番1号大

日本印刷株式会社内

(72) 発明者 林 昌弘

東京都新宿区市谷加賀町一丁目1番1号大

日本印刷株式会社内

(74) 代理人 弁理士 蛭川 昌信 (外7名)

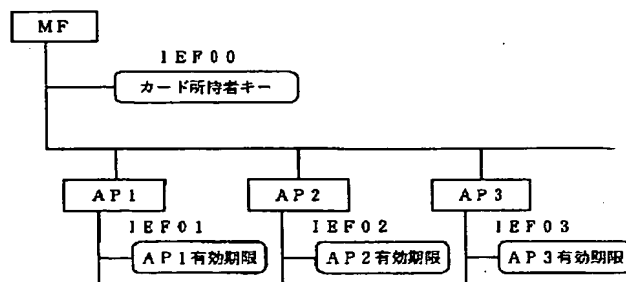
最終頁に続く

(54) 【発明の名称】 期限つきセキュリティステータスを有するICカード

(57) 【要約】

【課題】 真のカード所持者以外の人物によるICカードの継続的な不正利用を防止する。

【解決手段】 タイマー機能を有するICカードにおいて、カード所持者の認証終了後認証有効状態を示すセキュリティステータスが所定の時間だけ持続するようにしたもので、カード所持者認証の有効期限をマスターキーファイルIEF00、アプリケーションキーファイルIEF01、IEF02、IEF03に設定するようにしたものである。



【特許請求の範囲】

【請求項1】 演算装置、主メモリ、読み出し専用メモリ、不揮発性メモリ、タイマー機能を有するICカードにおいて、カード所持者の認証終了後認証有効状態を示すセキュリティステータスが所定の時間だけ持続するようにしたことを特徴とするICカード。

【請求項2】 上記所定の時間を経過した後、セキュリティステータスを元に戻す、あるいは該当するアプリケーションファイルを閉塞するようにしたことを特徴とするICカード。

【請求項3】 請求項1または2記載のICカードにおいて、カード所持者認証の有効期限をキーファイルに設定したことを特徴とするICカード。

【請求項4】 請求項1または2記載のICカードにおいて、アプリケーションファイル毎にカード所持者認証の有効期限をキーファイルに設定するようにしたことを特徴とするICカード。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】 本発明は真のカード所持者以外の人によるICカードの継続的な不正利用を防止するようにしたICカードに関する。

【0002】

【従来の技術】 図4に示すように、リーダ／ライタ1はICカード2に対してコマンド（命令）を送信し、これを受信したICカードは、コマンドを解釈して書き込み／読み出し等の処理を実行し、処理結果をレスポンスとしてリーダ／ライタ1へ返すようになっている。

【0003】 図5に示すように、ICカード2は、CPU2a、RAM2b、ROM2c、EEPROM2dを有しており、ROM2cに記憶されているプログラムをCPU2aに読み込み、リーダ／ライタ1から送信されるコマンドをI/Oポートを通して受信すると、コマンドとともに送信されたデータを読み込んで必要な処理を行い、結果をEEPROM2dの所定のファイルエリアに書き込み、I/Oポートを通してレスポンスを出力する。なお、2eはタイマーモジュールであり、CPU2aの動作とは独立に動作し、設定された時間が経過すると、CPU2aに対して割り込みをかけて通知する計時装置である。

【0004】 図6はアプリケーションプログラム用領域とオペレーティング・システム（OS）用領域からなるEEPROM3を示したもので、アプリケーション領域の先頭アドレスから、アプリケーションA、B、Cのファイルをこの順で割り当てるときに、同時に、ファイルエリアの割り当て順に、アプリケーション領域の最後から先頭に向かってAディレクトリ、Bディレクトリ、Cディレクトリが形成される。ディレクトリはファイルの制御情報であり、図7に示すように、ファイルを識別するためのファイルID、ファイルが記憶される先頭アドレ

ス、エリア容量、属性情報（リード／ライトのアクセス権（キー）の情報）、チェックコードからなっている。

【0005】 図6において、アプリケーションの領域に続いたOS用領域には、ディレクトリに示された先頭アドレスとエリア容量から、割り当てられたファイルエリアの最後のアドレスを示すポインタ、積み上げられた最後のディレクトリを示すポインタ等のOSが使うデータがセットされる。ポインタP、P'の間の領域がさらに割り当て可能なメモリ領域である。

【0006】 リーダ／ライタからのコマンドは、図8に示すように、コマンドの分類（CLA）、命令（INS）、パラメータP1、P2にデータ長Lcおよびデータ部（ファイルID、エリア容量、属性情報）が付加されたものであり、ファイルの割り当ては、クリエイト・ファイル命令で行われる。

【0007】

【発明が解決しようとする課題】 従来のICカードではカード所持者が端末から入力したキー（PIN: Personal Identification Number）をICカード内に格納されたキーと照合し、一致すればセキュリティステータスを更新するようにしたので、それ以降はICカードが非活性化（接続装置からカードが抜かれた状態）されるまではセキュリティ属性が満足されるレベルでファイルへのアクセスが可能であった。

【0008】 図9において、マスターファイル直下のキーファイルIEF00は、カード所持者キーを表し、AP1、AP2、AP3は専用ファイルDF内のアプリケーションプログラムファイルを示し、IEF01、IEF01、IEF03はそれぞれ各アプリケーションプログラムにアクセスするためのキーPIN1、PIN2、PIN3が格納されているキーファイルである。

【0009】 カード所持者の認証（グローバルセキュリティステータス）はMF直下のキーに対するPIN入力時に行われ、入力されたPINがIEF00のキーと一致すると、図10に示すグローバルステータスが0から1に更新され、それ以降はICカード利用システム側（接続装置側）で明示的にカード所持者の認証手続きを実施しない限り、あるいはICカード側で非活性化されない限り、最初のグローバルセキュリティステータスが保持される。

【0010】 この状態で、各専用ファイルにアクセスするための権限が与えられ、例えばアプリケーションAP1にアクセスする場合は、キーファイルIEF01のPIN1と照合し、これが合致すればAP1にアクセス可能となる。このとき図10のセキュリティステータスが0から1に更新される。なお、セキュリティステータスは当該アプリケーションファイルにアクセスできる権限であり、他のアプリケーションに対しては及ばない。

【0011】 このように、一旦認証手続きが成功する

と、最初のグローバルセキュリティステータスが保持されるため、カードの真正性の認証手続きをチャレンジ／レスポンスの交換（接続装置とICカード側とで相互に乱数を渡して相手が真正かどうかを確認する手続き）を行ったとしても、接続装置に向かって操作している人物が当初のPIN入力時に認証した正当なカード所持者から別の不正な操作者になっても検出する手段がなかった。

【0012】このように接続装置に向かって操作している人物が真正なカード所持者から不正な人物が変わってしまう状況としては、POSレジスター端末でのICカードの抜き忘れや携帯電話機にSIM（Subscriber Identification Module）のICカードを挿入したまま電話機に置き忘れる状況が想定される。

【0013】本発明は上記課題を解決するためのもので、真のカード所持者以外の人物によるICカードの継続的な不正利用を防止することを目的とする。

【0014】

【課題を解決するための手段】本発明は、演算装置、主メモリ、読み出し専用メモリ、不揮発性メモリ、タイマー機能を有するICカードにおいて、カード所持者の認証終了後認証有効状態を示すセキュリティステータスが所定の時間だけ持続するようにしたことを特徴とする。また、本発明は、上記所定の時間を経過した後、セキュリティステータスを元に戻す、あるいは該当するアプリケーションファイルを閉塞するようにしたことを特徴とする。また、本発明は、カード所持者認証の有効期限をキーファイルに設定したことを特徴とする。また、本発明は、アプリケーションファイル毎にカード所持者認証の有効期限をキーファイルに設定するようにしたことを特徴とする。

【0015】

【発明の実施の形態】以下、本発明の実施の形態について説明する。本発明のICカードは図5に示した構成のもと同様であり、タイマー機能を有している。このタイマー機能は外部から供給されたクロックを利用して経過時間を測定し、指定された有効期限の時間を経過したことをCPU2aに知らせる機構であり、専用ハードウェアで実現してもソフトウェアによるインターバルタイマーで実現してもかまわない。

【0016】本発明はセキュリティステータス（認証有効状態）に有効期限を設け、カード所持者のPIN入力によるカード所持者認証後のセキュリティステータスの有効状態が一定時間だけ継続し、一定時間経過後にセキュリティステータスがカード所持者認証前に戻ることににより、それ以降の継続的な使用はできないようにしたものである。以下で説明する例では有効期限の設定はグローバルセキュリティステータスと各アプリケーションのセキュリティステータスすべてに対して設定している

が、有効期限の設定はこれに限定されるものではなく、例えばグローバルセキュリティステータスのみ、あるいは各アプリケーションのセキュリティステータスに対して、あるいは特定の重要なアプリケーションのセキュリティステータスに対して設定する等適宜行うようにしてもよい。

【0017】図1に示すように、MF直下のキーファイルIEF00、各アプリケーションファイル下のキーファイルIEF01、IEF02、IEF03……にはそれぞれ有効期限のレコードが付いている。この有効期限は最初から設定されていても良いし、或いはその後必要性が生じた時に設定するようにしても良い。例えば、認証コマンドでMF直下のキーファイルIEF00を指定すると、入力されたPINとファイル内のキーの値を照合後、一致すれば現在のグローバルセキュリティステータスを記憶した後に、グローバルセキュリティステータスを更新すると共に、タイマー機能を開始させる。タイマー機能に対して指示する有効期限は、アプリケーションAP1を利用する場合には、IEF00の有効期限（カード全体の有効期限で、例えばあらかじめ設定）とIEF01に記録された有効期限の和または差等の四則演算によって求められるようにする。アプリケーションAP2を利用する場合にはIEF00とIEF02のそれぞれに記録された有効期限の和または差等の四則演算によって求められる。また、IEF00の有効期限も何らかの演算をして求めるようにしてもよい。このようにしてカード所持者認証の有効期限をアプリケーション毎に可変に設定しておくことができる。もちろん、各有効期限は他のどのような方法によって設定してもよい。

【0018】図2はカード所持者認証プロセスフローの例を示す図で、左側から右側に向かう矢印は端末側からICカードへのコマンド、右側から左側へ向かう矢印はICカードから端末側へ送られるレスポンスを示している。A1において、カード所持者がアプリケーションを選択し、A2において、AP1を選択するセレクトファイルコマンド（ファイル選択命令）をICカードに対して送り、正常終了の場合にはA3において、ICカード側からステータスワード（9000）をレスポンスとして返す。次にV1においてカード所持者がPINを端末に入力し、V2において、認証コマンド（パラメータ＝IEF00、IEF01、データ部＝カード所持者が入力したPIN）が送られ、V3において、ICカード側ではPINの照合、タイマーセットを行い、正常終了であればレスポンスとしてステータスワード（9000）を返す。この状態で、AP1へのアクセス権が得られ、P1以降アプリケーションに固有のプロトコルで相互のコマンド／レスポンスが行われる。この間にセキュリティステータス有効期限が経過すると、Pnにおいて、セキュリティステータスを満たさないため、ステータスワード6982が返され、カード所持者認証前へ戻るこ

になる。そして、さらに継続使用するためには、上記V1、V2のプロセスを実行しなければならない。

【0019】図3は認証コマンド処理の例を示す図で、AP1へのアクセス権を得る場合の処理フローを示している。認証コマンドでIEF00とIEF01を指定し、AP1へのアクセスを試みると、まずIEF00を検索し、IEF00が見つかったと、現在のセキュリティステータスをメモリ中に記憶し、コマンドのデータ部（カード所有者が入力したPINの値）とIEF00のレコード値を照合する（ステップS1～S4）。照合が一致すると、次にIEF01を検索し、IEF01が見つかったとセキュリティステータスの有効期限Tを算出する（ステップS5～S8）。次いで、タイマー機能を出し、引き数Tをタイマーに設定（有効期限の設定）する。次いで、レスポンスを編集し（ステップS10）、正常終了のレスポンスを返す（ステップS11）。こうして有効期限が設定されるので、この期限を経過するとセキュリティステータスを満たさなくなり、継続使用の場合には再度認証処理を行わなければならない。なお、ステップS5において、IEF00の照合が失敗した場合には、ステップS10に飛んでレスポンス内容を編集し、エラーを返す。

【0020】

【発明の効果】以上のように本発明によれば、真正なICカード所有者によるPIN入力認証後にICカードを挿入した端末装置が不正な利用者の手に渡った場合でも、不正利用者によるICカードの継続的な利用を阻止

することができる。ICカードを利用したシステムで特にカード所持者の認証を厳密に行わなければならないシステム、例えば電子現金システムにおいて、本発明のICカードを利用することにより、ICカード自体が定期的にセキュリティステータスをカード所持者のPINによる照合認証前の状態に戻してしまうので、仮に不正利用者の手に渡ったとしても重要な現金情報ファイルのセキュリティ属性を満足できなくなり、継続的な不正利用を阻止することができる。

【図面の簡単な説明】

【図1】 本発明のファイル構造を説明する図である。

【図2】 カード所有者認証プロセスフローの例を示す図である。

【図3】 認証コマンド処理の例を示す図である。

【図4】 リーダ/ライタとICカードの通信を説明する図である。

【図5】 ICカードの構成を説明する図である。

【図6】 EEPROMの構成を説明する図である。

【図7】 ディレクトリの構成を説明する図である。

【図8】 コマンドの構成を説明する図である。

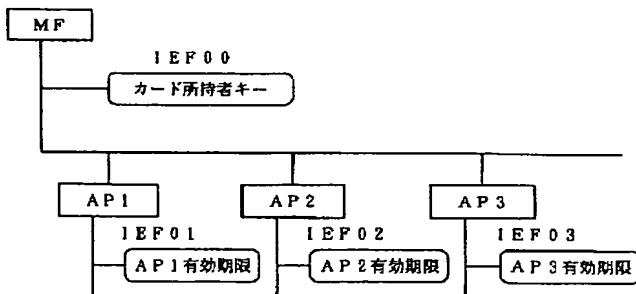
【図9】 ファイル構造を示す図である。

【図10】 セキュリティステータスを説明する図である。

【符号の説明】

1…リーダ/ライタ、2…ICカード、2a…CPU、2a…RAM、2b…ROM、2d…EEPROM、2e…タイマー。

【図1】

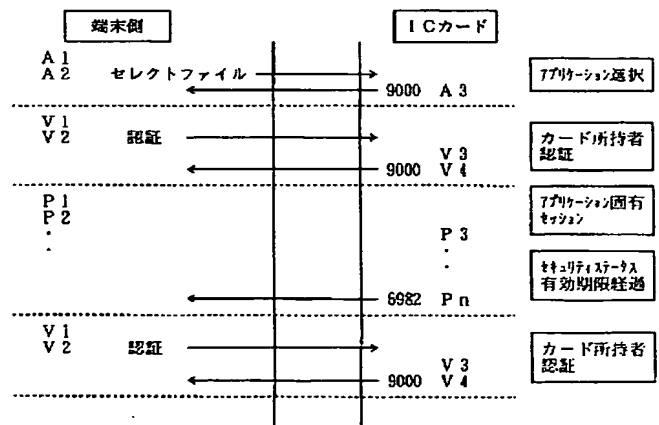


【図4】

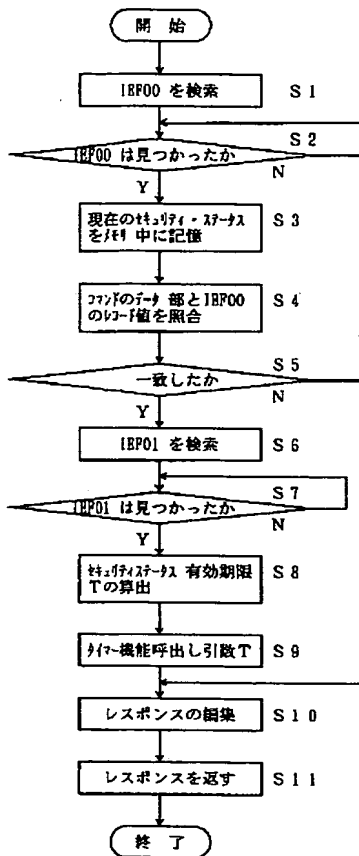


【図7】

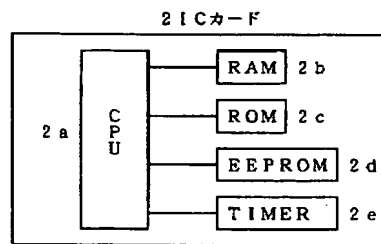
【図2】



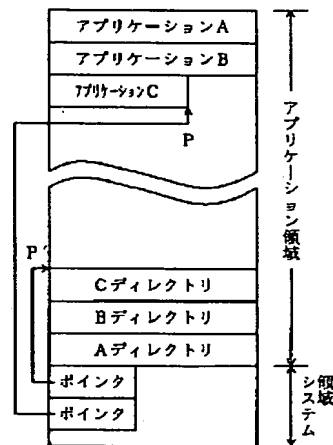
【図3】



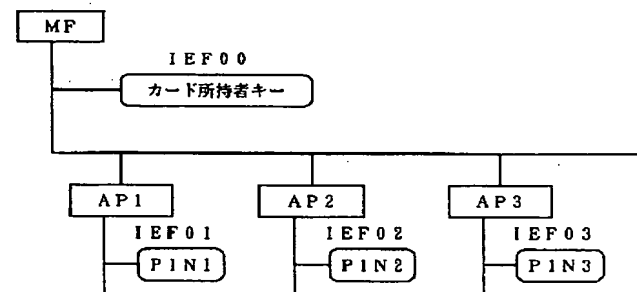
【図5】



【図6】



【図9】



【図8】

| CLA | INS | P1 | P2 | Lc | カードID | 記憶容量 | 属性情報 |
|-----|-----|----|----|----|-------|------|------|
|-----|-----|----|----|----|-------|------|------|

【図10】

| | |
|-------------|--------|
| グローバル・ステータス | 0 or 1 |
| セキュリティステータス | 0 or 1 |
| セキュリティステータス | 0 or 1 |
| ... | |

フロントページの続き

(72)発明者 牧野 寛

山形県山形市松波一丁目1番1号大日本山

形アイ・エス・ディー株式会社内